Mathematische Probleme.

Vortrag, gehalten auf dem internationalen Mathematiker-Kongreß zu Paris 1900.

Von

D. Hilbert.

10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.

Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*

$x_1^2 + x_2^2 + x_3^2 + x_4^2$

$\exists\, x_1 \dots x_n \in \mathbb{N} \quad p(x_1 \dots x_n) = 0$

$p \in \mathbb{Z}[x_1 \dots x_n]$

Def $X \subseteq \mathbb{N}^n$ ist diophantisch, wenn

$$X = \{(x_1 \dots x_n) \mid \exists\, y_1 \dots y_k \in \mathbb{N}\ p(x_1 \dots x_n, y_1 \dots y_k) = 0\}$$

$p \in \mathbb{Z}[x_1 \dots x_n y_1 \dots y_k]$

Satz: X diophantisch $\Rightarrow X$ r.e.

Thm: X diophantisch $\Leftrightarrow X$ r.e.

Cor H10 non ha soluzione

Dim ins. della formula

$$H = \{(x,y) \mid \exists z_1 \dots z_n \in \mathbb{N} \quad p(x,y,z_1,\dots z_n) = 0\}$$

Teo γ diof. $\Leftarrow$ $\times$ r.e.

Ins. diofantei

Es $\mathbb{N}$, $\varnothing$ $\quad \exists y \; x_1 + y + 1 - x_2 = 0$

$\{(x_1,x_2) \in \mathbb{N}^2 \mid x_1 < x_2\}$ "la rel $x_1 < x_2$"

$<$ $\quad$ $\leq$

$=$ $\quad$ $=$

$\neq$ $\quad$ $\neq$

$x \equiv y \ (z) \leftrightarrow \exists t_1 t_2 \quad x + z t_1 = y + z t_2$

Lem Gli ins. diof. sono chiusi per $\cup$

- $\cup$ $\quad (x_1 \dots x_n) \in A \rightsquigarrow \exists \bar{y} \; p(\bar{x},\bar{y}) = 0$

  $\bar{x} \in B \rightsquigarrow \exists \bar{z} \; q(\bar{x},\bar{z}) = 0$

  $\bar{x} \in A \cup B \leftrightarrow \exists \bar{y},\bar{z} \; p(\bar{x},\bar{y}) \cdot q(\bar{x},\bar{z}) = 0$

- $\cap$ $\quad \bar{x} \in A \cap B \rightsquigarrow \exists \bar{y},\bar{z} \; (p(\bar{x},\bar{y}))^2 + (q(\bar{x},\bar{z}))^2 = 0$

- proiezioni

- prodotti cartesiani

$$A \subseteq \mathbb{N}^n \qquad B \subseteq \mathbb{N}^k$$

$$A \times B = A \times \mathbb{N}^k \cap \mathbb{N}^n \times B$$

Es.

$x = y \bmod z$ $\Leftrightarrow$ $x \equiv y \ (z) \ \wedge \ x < z$

$x > y \operatorname{div} z$ esercizio.

Strategia

- $x^y = z$ è diofantea
- operazioni sulle sequenze sono diofantee
- computabilità (Turing) è diofantea.

$x^2 - y^2 = 3$ e' di Pell

- Eq. di Pell

$$P_a = \{ (x,y) \in \mathbb{Z}^2 \mid x^2 - (a^2-1) y^2 = 1 \}$$

$a \geq 1$

$(1,0)$, $(a,1) \in P_a$

$$(x,y) = x + y\sqrt{a^2-1}$$

- $x + y\sqrt{\ }$, $x' + y'\sqrt{\ } \in P_a$

$$(x + y\sqrt{\ })(x' + y'\sqrt{\ }) \in P_a$$

$$= xx' + yy'(a^2-1) + (xy' + yx')\sqrt{a^2-1}$$

- $(x + y\sqrt{\ })(x - y\sqrt{\ }) = 1 = (1,0)$

- $x_n(a) + y_n(a)\sqrt{a^2-1} = (a + \sqrt{a^2-1})^n$

$(x,y) \in P_a \cap \mathbb{N}^2 \iff \exists n \quad (x,y) = (x_n(a), y_n(a))$

- $$\begin{cases} x_{m+n}(a) = x_m(a) x_n(a) + y_m(a) y_n(a) (a^2-1) \\ y_{m+n}(a) = x_m(a) y_n(a) + x_n(a) y_m(a) \end{cases}$$

$$\begin{cases} x_{m\pm1}(a) = a \cdot x_m(a) \pm (a^2-1) y_m(a) \\ y_{m\pm1}(a) = a\, y_m(a) \pm x_m(a) \end{cases}$$

$$\begin{cases} x_{n+1}(a) = 2a\, x_n(a) - x_{n-1}(a) \\ y_{n+1}(a) = 2a\, y_n(a) - y_{n-1}(a) \end{cases}$$

$$a^n \le x_n(a) \le (2a)^n$$

Lemma

α. $x_n(a)$ e $y_n(a)$ sono crescenti in n

β. $a^n \le x_n(a) \le (2a)^n$

γ. $\mathrm{mcd}\left(x_n(a), y_n(a)\right) = 1$

δ. $y_m(a) \mid y_n(a) \iff m \mid n$

$\Leftarrow$ $y_{k+m} = y_k x_m + y_m x_k$

$\Rightarrow$ $y_m \mid y_n$ $\quad n \bmod m = n_0 \neq 0$

$y_m \mid y_{n_0} \rightsquigarrow y_{n_0} < y_m$

- $y_{nk}(a) \equiv k\left(x_n(a)\right)^{k-1} y_n(a) \quad \left(\bmod \left(y_n(a)\right)^3\right)$

$$x_{nk} + y_{nk}\sqrt{\ } = \left(x_n + y_n\sqrt{\ }\right)^k$$

$$= x_n^k + k x_n^{k-1} y_n \sqrt{\ } + \dots$$

$$y_{nk}(a) \equiv k \left(x_n(a)\right)^{k-1} y_n(a) \quad (\mathrm{mod}\ (y_n(a))^3)$$

ε. $(y_n(a))^2 \mid y_{n\, y_n(a)}(a)$

$$(y_n(a))^2 \mid y_t(a) \longrightarrow y_n(a) \mid t$$

ζ. $y_n(a) \equiv n \quad (a-1) \qquad y_n(a) \equiv n \quad (2)$

η. $a \equiv b \ (c) \rightarrow x_n(a) \equiv x_n(b) \ (c) \ \wedge \ y_n(a) \equiv y_n(b) \ (c)$

ϑ. $\underbrace{x_n(a) - y_n(a)(a-z)}_{t_n} \equiv z^n \quad (2az - z^2 - 1)$

$$t_{n+1} \equiv 2a\, t_n - t_{n-1} \qquad z^{n+1} \equiv 2a z^n - z^{n-1} \quad (\text{——})$$

$$z^{n-1}(z^2 - 2az + 1) \equiv 0 \quad (\text{——})$$

- $x_{2n \pm k}(a) \equiv -x_k(a) \quad (x_n(a))$

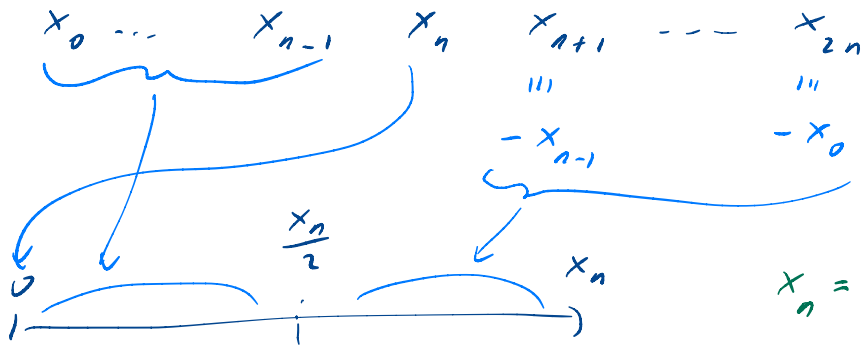
$$x_{n+n\pm k} \equiv (a^2-1)\, y_n\, y_{n+k} \equiv \underbrace{(a^2-1)\, y_n\, y_n}_{x_n^2 - 1}\, x_k \equiv -x_k \quad (x_a)$$

$< n$

- $0 \le i, j \le 2n$

$$x_i(a) \equiv x_j(a) \quad (x_n(a)) \longrightarrow i = j$$

eccetto $a = 2 \quad n = 1 \quad i, j = 0, 2$



$$x_n = a\,x_{n-1} + (a^2-1)\,y_{n-1}$$

1. $0 < i \le n$ $\quad x_J(a) \equiv x_i(a)$ $\quad (x_n(a))$

$$\Downarrow$$

$$J \equiv \pm i \quad (q\,n)$$

dim. tsnaciz.

Lemma $\quad 0 < N \qquad 1 < x$

$x = x_\mu(a)$ se e solo se c'è una sol. di

A $\quad (x,y) \in \mathcal{P}_a \qquad (u,v) \in \mathcal{P}_a \qquad (s,t) \in \mathcal{P}_b$

B $\quad b \equiv a \;(v) \qquad s \equiv x \;(v)$

C $\quad y^2 \mid v$

D $\quad b \equiv 1 \;(4y) \qquad t \equiv k \;(4y)$

E $\quad k \le y \qquad 1 < a < b \qquad 1 \le v \qquad x \in v$

1. A $x = x_i(a)$ $\quad y = y_i(a)$

$v = x_n(a)$ $\quad w = y_n(a)$

$s = x_j(b)$ $\quad t = y_j(b)$

$i = k$

2. B $b \equiv a \quad (x_n(a))$ $\qquad x_j(b) \equiv x_i(a) \quad (x_n(a))$

$\parallel \qquad \parallel$

$x_j(b) \equiv x_j(a) \quad (x_n(a))$

n

c

$j \equiv \pm i \quad (4n)$

3. C + 2

$(y_i(a))^2 \mid y_n(a) \xrightarrow{\varepsilon} y_i(a) \mid n$

$j \equiv \pm i \quad (4 y_i(a))$

4. D + 3 $\qquad b \equiv 1 \quad (4 y_i(a))$ → 5

$k \equiv y_j(b) \equiv j \quad (4 y_i(a))$

5. $k \equiv \pm i \quad (4 y_i(a))$

↘

6. $k \leq y_i(a) \longrightarrow k = i$ ☺

$a \to i \leq y_i(a)$ ↗

Se $x = x_k(n)$

$x = x_k(n)$ $\quad$ $y = y_k(a)$

$u = x_n(a)$ $\quad$ $v = y_n(a)$ $\quad$ $n = 2k\, y_k(a)$

$s = x_k(b)$ $\quad$ $t = y_k(b)$

$$\begin{cases} b \equiv a & (u) \\ b \equiv 1 & (4y) \end{cases}$$

e b grande abbastanza.

<u>Lemma</u> $m = z^k$ se e solo se ha soluzione

$x = x_k(a)$ $\quad$ $y = y_k(a)$

X $\quad x - y(a - z) \equiv m \quad (2az - z^2 - 1)$

Y $\quad a^2 - (w^2 - 1)(w-1)^2 t^2 = 1$

Z $\quad m < 2az - z^2 - 1 \quad z < w \quad k < w$

$\varnothing \quad x_n(a) - y_n(a)(a - z) \equiv z^n \quad (2az - z^2 - 1)$

1. X $\quad m \equiv z^k \quad (2az - z^2 - 1)$

2. Y $\quad a = x_J(w) \quad (w-1)t = y_J(w)$

$$\begin{matrix} & & ||| & & ||| & \xi \\ w - 1 \leq J & \Leftarrow & 0 & & J & (w-1) \end{matrix}$$

3. $\xi^\kappa < \omega^{\omega \cdot 1} \leq \chi_f(\omega) = a$

$\xi^\kappa \leq 2a\xi - \xi^2 - 1$

4. $la \equiv \dot{a} \quad u_n = \quad \kappa \quad m = \xi^\kappa.$

← facile.